Romain Jacquet **BTS SIO 1**
26/11/2025

Compte Rendu Atelier 10 : TP2
Sécurité informatique

Sommaire

Introduction

Ce TP sur la sécurité informatique portait sur les risques liés aux clés USB dans l'entreprise. L'objectif était d'apprendre à identifier les dangers, proposer des solutions et les présenter aux décideurs. À travers quatre phases pratiques, j'ai découvert comment concilier sécurité et efficacité au travail.

Phase 1

Ce que j’ai retenu

Le document du CNRS m’a rappelé les 5 grands principes de la sécurité : confidentialité, intégrité, disponibilité, traçabilité et preuve. Pour GSB, ça veut dire qu’il faut protéger nos secrets, garantir que les résultats des essais cliniques ne soient pas modifiés, et pouvoir retracer toutes les actions pour les audits.

Le documentaire *"La guerre invisible"* d’Arte m’a un peu stressé : ça parle de cyberattaques et de vol de données. Ça m’a bien confirmé qu’on ne rigole pas avec la sécurité.

Le CERTA et les référentiels métiers m’ont aidé à comprendre qui fait quoi dans une équipe de sécurité.

Mon analyse des risques chez GSB :

- Les chercheurs utilisent encore beaucoup de clés USB perso (42% !).

- Il y a un risque que des données sensibles (formules, résultats d’essais, etc.) fuient, ce qui pourrait coûter des millions et détruire la confiance dans notre labo.

- Si GSB ne respecte pas les normes (FDA, EMA), ça pourrait entraîner de grosses amendes.

Phase 2

Référence :	NOTE-RISQUES-USB-2024	**De :**	Direction des Systèmes d'Information
Date :	26 novembre 2024	**À :**	Direction Générale, Comité de Direction
Objet :	Risques liés aux clés USB et mesures proposées	**Pièces jointes :**	Aucune

1. CONTEXTE ET CONSTAT

Situation actuelle

L'utilisation de clés USB au sein de GSB présente des risques cyber importants, notamment en raison de la sensibilité des données de recherche pharmaceutique et des exigences réglementaires (RGPD, bonnes pratiques de laboratoire).

Données d'analyse

Plus de 60 % des incidents de sécurité dans le secteur de la santé ont pour origine un support amovible non contrôlé. Chez GSB, plusieurs incidents mineurs liés à des clés USB non chiffrées ont été remontés au cours des 6 derniers mois.

2. ANALYSE

Éléments identifiés

Trois risques majeurs ont été identifiés :

Perte ou vol de données sensibles — HAUTE

Les clés USB non sécurisées exposent GSB à des fuites de données stratégiques (formules, essais cliniques, informations patients).

Introduction de programmes malveillants — MOYENNE

Les clés USB peuvent servir de vecteur à des virus ou rançongiciels, avec un impact potentiel sur la continuité des activités.

Non-conformité réglementaire — FAIBLE

L'absence de politique claire concernant les supports amovibles pourrait être sanctionnée par les autorités de santé.

3. RECOMMANDATIONS

Propositions d'action

Il est recommandé de :

- Généraliser le chiffrement des supports amovibles
- Sensibiliser les collaborateurs aux risques cyber
- Intégrer ces règles dans la charte informatique de GSB

Plan d'action proposé

Action prioritaire 1

Responsable: DSI Échéance: 31/12/2024 HAUTE

Interdire l'usage de clés USB personnelles et fournir des modèles chiffrés homologués.

Action prioritaire 2

Responsable: RH Échéance: 15/01/2025 MOYENNE

Organiser une campagne de sensibilisation sur les risques cyber et les bonnes pratiques.

Action complémentaire

Responsable: Juridique Échéance: 28/02/2025 FAIBLE

Mettre à jour la charte informatique pour inclure les règles d'usage des clés USB.

4. CONCLUSION

La sécurisation des supports amovibles est un enjeu critique pour la protection du patrimoine data de GSB et pour le respect de nos obligations légales. Les mesures proposées permettront de réduire significativement les risques identifiés.

Prochaines étapes : Validation de cette note par la Direction, puis lancement du plan d'action sous l'égide de la DSI.

Pour le service émetteur	Vu et approuvé
[NOM Prénom]	**[NOM Prénom]**
Directeur des Systèmes d'Information	Directeur Général Délégué

Phase 3

Jeu de rôle 1

VOUS Animateur de la Réunion

Stagiaire DSI GSB - Jeu de Rôle 1

Temps de préparation recommandé : 15 minutes

Votre Mission

Contexte : Vous présentez les recommandations de sécurité suite à un incident lié aux clés USB devant le comité de direction de GSB.
Objectif principal : Obtenir l'approbation du comité pour la mise en œuvre des mesures de sécurité.

Style de communication	Principal défi	Attitude
Professionnel & Convaincant	**Sécurité vs Productivité**	**Diplomatique & Ferme**

Questions de Préparation

Quels sont les 3 arguments principaux que vous utiliserez pour convaincre le comité de l'urgence des mesures ?

1. **Risque réglementaire :** Une fuite de données compromettrait nos certifications FDA/EMA et entraînerait des sanctions financières importantes.

2. **Protection de la propriété intellectuelle :** Nos recherches représentent des investissements de plusieurs millions d'euros qui doivent être protégés contre la concurrence.

3. **Réputation et confiance :** Un incident de sécurité pourrait nuire gravement à notre image auprès des autorités et partenaires.

Comment allez-vous présenter l'incident récent sans créer de panique mais en montrant la gravité ?

"L'incident récent nous a montré une vulnérabilité dans notre système. Heureusement, nous l'avons détecté à temps, mais il nous rappelle l'importance de renforcer nos protocoles. Dans notre secteur, une seule faille peut avoir des conséquences considérables sur des années de recherche."

Quelles objections anticipez-vous de chaque directeur et comment y répondrez-vous ?

Directeur Recherche : "Ça va ralentir nos projets" → "Nous avons prévu des solutions alternatives qui maintiennent votre productivité"

Directeur Opérations : "Trop contraignant pour le personnel" → "Période de transition progressive avec support dédié"

Directeur Qualité : "Est-ce suffisant pour les audits ?" → "Ces mesures répondent directement aux exigences FDA 21 CFR Part 11"

Quels compromis êtes-vous prêt à faire sans sacrifier l'essentiel de la sécurité ?

-Accepter une période de transition de 2 mois plutôt que 1 mois
- Proposer des exceptions contrôlées pour les projets urgents avec validation hiérarchique
- Maintenir l'utilisation des clés USB cryptées pour certains usages spécifiques sous supervision

Comment allez-vous gérer un directeur particulièrement réticent ?

"Je comprends parfaitement vos préoccupations. Pouvez-vous nous préciser quels aspects vous semblent les plus problématiques ? Nous pourrions peut-être trouver des ajustements spécifiques pour votre département tout en maintenant le niveau de sécurité nécessaire."

Préparation des Interventions

Votre introduction (2-3 minutes)

"Bonjour à tous, je vous remercie d'être présents. Aujourd'hui, je vais vous présenter les mesures de sécurité que nous devons mettre en place suite à l'incident récent. L'objectif est de protéger nos actifs les plus précieux : nos données de recherche et notre propriété intellectuelle, tout en maintenant notre efficacité opérationnelle."

Votre conclusion et appel à décision

"En conclusion, je propose que nous adoptions ces trois mesures prioritaires : 1) le déploiement de solutions de stockage sécurisées, 2) la formation obligatoire du personnel, et 3) l'audit régulier de nos procédures. Je sollicite votre approbation pour une mise en œuvre progressive sur les 8 prochaines semaines."

Exemples de réponses aux objections

Directeur Recherche : "Ça va ralentir nos projets !"

"Je comprends votre préoccupation. En réalité, ces mesures vont protéger nos avancées et éviter des retards bien plus importants en cas de fuite de données. Nous avons testé les solutions alternatives et elles n'ajoutent que quelques minutes par jour aux processus existants."

Directeur Opérations : "C'est trop contraignant !"

"Nous avons prévu une période de transition et des solutions alternatives qui simplifient les procédures. De plus, le service DSI fournira un support dédié pendant les premières semaines pour accompagner votre équipe."

Checklist de Préparation

- [x] J'ai relu ma note professionnelle et connais parfaitement mes recommandations
- [x] Je maîtrise les spécificités du secteur pharmaceutique (FDA, EMA, propriété intellectuelle)
- [x] J'ai anticipé les objections de chaque participant et préparé mes réponses
- [x] Je suis prêt à proposer des compromis réalistes
- [x] Je me suis entraîné à respecter le timing (20 minutes total)

Phase 4

1. Email à tous les collaborateurs

Objet : [URGENT] Nouvelle politique de sécurité pour les clés USB

Chers collaborateurs,

Dans le cadre de nos efforts pour protéger la propriété intellectuelle de GSB et garantir notre conformité aux normes réglementaires, nous avons mis en place une nouvelle politique concernant l'utilisation des clés USB.

Interdiction : L'utilisation de clés USB personnelles est désormais formellement interdite.
Solution : À partir de maintenant, il sera obligatoire d'utiliser uniquement les clés USB fournies par l'entreprise. Ces clés sont chiffrées et toutes les données transférées seront automatiquement journalisées. Une formation obligatoire sera lancée pour vous expliquer ces nouvelles règles (voir le plan ci-dessous).

2. Modifications apportées à la Charte GSB

Afin de renforcer la sécurité et la conformité, nous avons modifié plusieurs articles de la Charte GSB, comme suit :

Article 4 (Utilisation des clés USB) :

- Nous avons ajouté l'obligation de journaliser systématiquement tous les transferts de données (audit trail) pour nous conformer à la norme FDA 21 CFR Part 11.

Article 11 (Formation et Sensibilisation) :

- Désormais, les formations couvriront spécifiquement les risques liés aux périphériques USB et les attaques d'ingénierie sociale, afin de mieux gérer les vulnérabilités humaines.

Article 13 (Sanctions) :

- Toute utilisation non conforme des clés USB entraînera des sanctions disciplinaires immédiates, en raison des risques importants liés au vol de formules et de brevets.

3. Plan de déploiement progressif

Le déploiement des nouvelles règles se fera en plusieurs étapes, selon le planning suivant :

- Phase pilote (J+15) : Lancement du plan de support et validation des solutions techniques. La phase pilote démarrera dans le département R&D et durera entre 30 et 45 jours.

- Formation initiale (J+60) : Tous les collaborateurs devront suivre la formation obligatoire d'ici 60 jours.

- Déploiement total (J+90) : Blocage des ports USB non autorisés sur l'ensemble du réseau GSB. Cette étape marquera la fin de la phase de substitution contrôlée.

4. Fiche d'auto-évaluation

- Qualité de la note : Très satisfaisante. J'ai respecté le format de la note interne (version du 26/11/2025) et structuré l'analyse autour des risques majeurs pour la propriété intellectuelle et la conformité.

- Communication (jeu de rôle) : Bonne maîtrise. J'ai su répondre aux objections en expliquant que le coût d'adaptation est bien inférieur au risque de perdre un brevet, et j'ai proposé une solution de compromis, avec une prolongation de la phase pilote.

- Point d'amélioration : Même si j'étais bien préparé, je dois m'assurer de toujours mettre en avant l'argument de la conformité légale, surtout face à un directeur réticent.

Conclusion

Ce travail m'a montré l'importance de sécuriser les clés USB pour protéger les données de l'entreprise. J'ai appris à analyser des risques et à défendre des solutions de sécurité de manière convaincante. Cette expérience m'a fait comprendre que la sécurité informatique est l'affaire de tous dans une organisation.